special report entitled "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues", CERT Coordination Center. Among all the other techniques that this paper describes, a hop-by-hop trace back scheme is discussed. This mechanism consists of a manual and tedious process by which a network administrator gathers information on each router on the upstream path of the flow being traced one step at a time until the source is reached.

[006] Other prior art solutions involve systems where routers are requested to insert their IP addresses, or other unique identifiers, into the IP packet headers. The victim of an attack reconstructs the path by using the information gathered by correlating all the received, marked datagrams. This system is described by S. Savage, D. Wetherall, A. Karling and T. Anderson in "Practical Network Support for IP Trace back", SIGOMM'00, Stockholm, Sweden.

[007] Another back-tracing method is iTrace, which relies on routers sending a new type of Internet control message protocol (ICMP) message to the destination of the datagram examined with a certain probability. By gathering a given number of these messages the receiver of a certain flow can reconstruct the path to the source. This method is described by S. Bellovin, M. Leech, T.Taylor, "ICMP Trace back messages", IETF work in progress.

[008] Finally, the third classical approach is to rely on routers keeping track of all packets they forward in some efficient matter. In a hash-based solution every router keeps a table containing a hashed value from every packet forwarded during a given interval. If a particular flow is to be traced, routers on the upstream path forward their tables to an entity that will carry out a correlation process to determine the next hop. The method relies on Bloom filters to speed up the look-up process in the table. This method was described by C. Snoeren, C. Patridge, L. Sanchez et al., "Hash-based IP Trace back", SIGCOMM'01, San Diego.

10/635,602

FA
11/17/2008

[009] The Applicant's co-pending US Patent Application SN: ~~N/A~~, filed August 7, 2003 for a "Mechanism for Tracing-back Anonymous Network Flows in